

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of: Ralph Samuel HOEFELMEYER et al. Application No.: 09/911,592 Filed: July 24, 2001 Attorney Docket: COS00019 Client Docket: 09710_1007	Group Art Unit: 2131 Examiner: Chen, S.
--	--

For: NETWORK SECURITY ARCHITECTURE

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated November 29, 2007.

I. REAL PARTY IN INTEREST

Verizon Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There is a related Appeal in Application Serial No. 10/024,202.

III. STATUS OF THE CLAIMS

Claims 1-15 are pending in this appeal. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-15 on November 2, 2007, the claims having been twice-rejected.

IV. STATUS OF AMENDMENTS

The amendment to claims 1-15 filed August 15, 2007 has been entered and the claims on appeal are the same claims presented in that amendment.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent system claim 1.

Independent claim 1 is directed to a network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.*, Specification ¶ 4 and FIG. 1) The claimed system comprises a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code. (*See, e.g.*, Specification ¶¶ 5, 14, 22 and 25) The claimed system comprises an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets. (*See, e.g.*, Specification ¶¶ 5, 27-29 and 30) The claimed system comprises a switch coupled between the internet backbone (*See, e.g.*, Specification ¶¶ 5, 15, 16, 19, 20, 33 and 34) the scanning system, and the anti-virus server, said switch configured for directing incoming electronic mail from the internet backbone to the scanning system. (*See, e.g.*, Specification ¶¶ 5, 15, 19, 20-26, 32, 36)

Independent system claim 3.

Independent claim 3 is directed to a network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.*, Specification ¶ 4 and FIG. 1) The claimed system comprises a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code. (*See, e.g.*, Specification ¶¶ 5, 14, 22 and 25) The system comprises a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code (*See, e.g.*, Specification ¶¶ 16, 20, 21 and 25) and directing the incoming electronic mail to the scanning system when the incoming electronic mail is determined to be scanned for malicious code. (*See, e.g.*, Specification ¶¶ 20 and 25) The claimed system comprises an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets. (*See, e.g.*, Specification ¶¶ 5, 27–29 and 30) The system further comprises a switch coupled between the internet backbone, the scanning system (*See, e.g.*, Specification ¶¶ 5, 15, 16, 19, 20, 33 and 34), and the anti-virus server, said switch configured for directing incoming electronic mail from the internet backbone to the mail proxy server. (*See, e.g.*, Specification ¶¶ 5, 15, 19, 20–26, 32, 36)

Independent system claim 5.

Independent claim 5 is directed to a network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.*, Specification ¶ 4 and FIG. 1) The claimed system comprises a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code. (*See, e.g.*, Specification ¶¶ 5, 14, 22 and 25) The system comprises a plurality of anti-virus servers coupled

to the intranets for downloading anti-virus code to clients coupled to the intranets. (*See, e.g.*, Specification ¶¶ 5, 14, 16, 19 and 21–23) The system further comprises a plurality of switches coupled between the internet backbone (*See, e.g.*, Specification ¶¶ 5, 15, 16, 19, 20, 33 and 34), the scanning systems, and the anti-virus servers, said switches configured for directing incoming electronic mail to at least one of the scanning systems. (*See, e.g.*, Specification ¶¶ 5, 15, 19, 20–26, 32 and 36)

Independent method claim 8

Independent claim 8 is directed to a method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.*, Specification ¶ 4 and FIG. 1) The claimed method comprises directing incoming electronic mail from the internet backbone to a scanning system. (*See, e.g.*, Specification ¶¶ 05, 15, 20, 25 and 28) The method comprises scanning incoming electronic mail for malicious code. (*See, e.g.*, Specification ¶¶ 16, 20, 21 and 25) The claimed method further comprising downloading anti-virus code to clients coupled to the intranets. (*See, e.g.*, Specification ¶¶ 5, 27–29 and 30)

Independent method claim 10

Independent claim 10 is directed to a method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone. (*See, e.g.*, Specification ¶ 4 and FIG. 1) The claimed method comprises directing incoming

electronic mail from the internet backbone to one of a plurality of mail proxy servers at the one of the mail proxy servers. (*See, e.g.*, Specification ¶¶ 16, 20 and 25) The method comprises determining whether the incoming electronic mail is to be scanned for malicious code. (*See, e.g.*, Specification ¶¶ 16, 20, 21 and 25) The method comprises directing the incoming electronic mail to a scanning system when the incoming electronic mail is determined to be scanned for malicious code; at the scanning system (*See, e.g.*, Specification ¶¶ 05, 15, 20, 25 and 28), scanning incoming electronic mail for malicious code. (*See, e.g.*, Specification ¶¶ 5, 21, 23, 25 and 26) The method further comprises downloading anti-virus code to clients coupled to the intranets. (*See, e.g.*, Specification ¶¶ 5, 27–29 and 30)

Dependent claims argued separately. (claims 2, 4, 7, 9, 6-11 and 12-15)

In addition to the switch, a Denial of Service (DoS) or Distributed DOS scanning/filtering switch may be employed to prevent these specific attacks. In one embodiment, a decoy server is also provided for masquerading as a legitimate server and logging suspicious activity from communications received from the internet backbone. (*See, e.g.*, specification, ¶ 05, claims 2, 4, 7, and 9)

In the architecture illustrated in FIG. 1, one or more front-end switches 110 are coupled to the Internet backbone 100 and provide the basic gate-keeping functionality of the architectures. In one implementation, the front-end switches 110 also measure and record the communications traffic between the customers' systems and the Internet for billing purposes. The front-end switches 110, which may be implemented with one or more CISCO™ 6509 switches, are thus responsible for receiving communications from the Internet backbone 110, directing the Internet communication to an appropriate security server for detecting and responding to incoming

threats, and load balancing among the security servers. (*See, e.g.*, specification, ¶ 15, claims 1-11) Accordingly, the front-end switches 110 are positioned to intercept incoming electronic mail and other communications before they are routed to the customers' systems. The switches are also connected directly to DoS/DdoS scanning/filtering switches operating at line speed. (*See, e.g.*, specification, ¶ 15)

A local area network 120, such as a fast ETHERNET™ network, couples the front-end switches 110 with the security servers, which comprise, for example, one or more mail proxy servers 130, one or more antivirus scanning servers 140, one or more client antivirus servers 150, one or more decoy servers 160, and a quarantine server 170. The front-end switches 110, the mail proxy servers 130, the antivirus scanning servers 140, the client antivirus servers 150, and the decoy servers 160 are in communication with a hub 180, which communicates with client intranets 190 that belong to respective customers. (*See, e.g.*, specification, ¶ 16, claims 1-15)

When the electronic mail message is received by one or more of the antivirus scanning servers 140, the electronic mail message is scanned for malicious code (step 209). In one implementation, antivirus scanning software on the one or more of the antivirus scanning servers 140 employs a catalog of viral signatures, which are often simple strings of bytes that are expected to be found in every instance of a particular virus. Usually, different viruses have different signatures, and the antivirus scanning software use signatures to locate specific viruses. To improve coverage, antivirus scanning software from multiple vendors may be employed, and the scanning may be performed on respective antivirus scanning servers 140 for improved performance. (*See, e.g.*, specification, ¶ 22)

If the electronic mail message is infected, tested at step 211, then the antivirus scanning server 140 may attempt to repair the infected portion of the electronic mail message, e.g., an

attachment (step 213), as determined by policy. If the electronic mail message or its attachment cannot be repaired (tested at step 215), then the electronic mail message is quarantined (step 217) by transferring the original, infected electronic mail message to the quarantine server 170 and by removing the infected portion from the electronic mail message to create a sanitized electronic mail message; this action may be varied by policy. The infected electronic mail message can be analyzed at the quarantine server 170 to study the virus, e.g., to generate a new viral signature or determine a new way to sanitize or repair a file infected with the virus. (*See, e.g.*, specification, ¶ 23, claims 12-15)

In either case, when the electronic mail message is infected, the sender and recipient of the electronic mail message may be notified of the detection of the viral infection (step 219), as determined by policy. This notification may be performed by appending text explaining the viral infection to the body of the electronic mail message or as a new attachment or even by composing and sending a new electronic mail message to the sender and recipient of the infected electronic mail message. (*See, e.g.*, specification, ¶ 24)

When the electronic mail message has been sanitized, by passing the antiviral scan (step 209), being repaired (step 213), or being quarantined (step 217), the sanitized electronic mail message is directed to the recipient, via hub 180 and the appropriate intranet 190. Accordingly, a scalable, resilient server-side antivirus scanning architecture is described, in which preferably multiple mail proxy servers 130 and antivirus scanning servers 140 are deployed to catch and sanitize incoming electronic mail messages. When malicious code is detected, an event is generated to the security management system. (*See, e.g.*, specification, ¶ 25, claims 12-15)

If, on the other hand, the incoming communication is not authorized (tested in step 405), then execution proceeds to step 407 where the incoming communication is routed to one of one

or more decoy servers 160. A decoy server 160 is a computer system that is configured to look like the client's computer system. Thus, when the unauthorized communication is routed to the decoy server 160, the decoy server 160 simulates the client's computer system (step 409). Because the decoy server 160 is separate from the client's computer system, any activity at the decoy server 160 performed by the intruder will not affect the client's computer system. In one aspect, the decoy server 160 also includes some un-patched operating system/application holes to look more appealing or breakable to a would-be intruder.

When the intruder takes the bait of the decoy server 160, all actions and keystrokes of the intruder are logged to the administration console 161 (step 411). Consequently, the intruder's action can be studied to understand the nature of the intrusion and learn how to counter the intrusion or to ascertain the source of the intrusion. In addition, an electronic mail alert can be sent from the administration console 161 to an operator to inform that a penetration attempt is underway. (See, e.g., specification, ¶¶ 32-36, claims 2, 4, 7, and 9)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 3, 5, 8, and 10 are properly provisionally rejected under obviousness-type double patenting over claims 1, 4, 7, 11, and 14 of co-pending Application Serial No. 10/024,202?

Whether claims 1, 3, 5, 6, 8, and 10-15 are obvious under 35 U.S.C. § 103 based on *Hypponen et al.* (US 2003/0191957) in view of *Yanovsky* (US 7,010,807)?

Whether claims 2, 4, 7, and 9 are obvious under 35 U.S.C. § 103 based on *Hypponen et al.* (US 2003/0191957) and *Yanovsky* (US 7,010,807) in view of *Network Associates, Inc (NAI)*?

VII. ARGUMENT

A. CLAIMS 1, 3, 5, 8, AND 10 ARE NOT OBVIOUS OVER CLAIMS 1, 4, 7, 11, AND 14 OF CO-PENDING APPLICATION SERIAL NO. 10/024,202

Whereas instant claims 1, 3, 5, 8, and 10 are silent as to any security manager and the taking of any action responsive to detection of a malicious code, claims 1, 4, 7, and 14 of co-pending Application Serial No. 10/024,202 recite that “in response to detection of an instance of malicious code, generating and transmitting an event indicating the detection to a security manager.” Claim 11 of the co-pending application recites that “in response to detection of an instance of malicious code, generating an event indicating the detection.”

The Examiner fails to indicate in the final rejection specifically why the subject matter of each of instant claims 1, 3, 5, 8, and 10, with the differences over claims 1, 4, 7, 11, and 14 of Application Serial No. 10/024,202, as indicated *supra*, would have been obvious over claims 1, 4, 7, 11, and 14 of Application Serial No. 10/024,202. Therefore, the Examiner has failed to present a *prima facie* case regarding the obviousness of the instant claimed subject matter.

The Examiner’s rationale for the obviousness-type double patenting rejection, as it appears at pages 2-3 of the latest Office Action of November 2, 2007, reads, *in toto*, as follows:

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows: co-pending applications and present application disclose a scanning system, an anti-virus server, and a switch for performing the same virus protection procedures. The instant claims are broader in scope to the claims for co-pending application and are therefore obvious/anticipated from them.

Merely because both applications claim “a scanning system, an anti-virus server,

and a switch for performing the same virus protection procedures” is insufficient to establish obviousness-type double patenting because such reasoning does not take into account other, differing, features of the claims in each application. For example, claim 1 of the co-pending application requires “generating and transmitting an event indicating the detection to a security manager” while instant claim 1 does not require this limitation.

The Examiner cites *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) for the proposition that an earlier species disclosure in the prior art defeats any generic claim, contending that the generic invention described in the present claims is anticipated by the species of the invention set forth in the claims of the co-pending application Serial No. 10/024,202. However, the *Titanium* case dealt with a titanium alloy and an anticipation issue, rather than obviousness-type double patenting. Moreover, genus/species obviousness analyses of the type proffered by the Examiner generally have less applicability to electrical cases than to chemical cases. What the Examiner is apparently arguing is that the instant claims are broader than the co-pending claims, so they must, *per se*, be obvious thereover. That is flawed reasoning as Applicants are unaware of any *per se* rule of obviousness. The determination of obviousness must be addressed on a case-by-case basis. While there may be instances in which broader subject matter may be obvious over more narrowly defined subject matter, it is **not always** the case. For example, there is no requirement in the instant claims 1, 3, 5, 8, and 10 that upon detection of a virus an administrator or security personnel **must** be notified of such detection, as is required by co-pending claims 1, 4, 7, 10, and 14. In the absence of evidence to the contrary, and the Examiner has proffered no such evidence, one cannot reasonably conclude that it would have been obvious, from a teaching of responsive to the detection of a malicious code, generating and transmitting an event indicating the detection to a security manager, to **not** generate and transmit

such an event to a security manager, or vice versa. Where the prior art (the co-pending claims in this case) teaches that an administrator or security personnel is notified of any detection of an instance of malicious code, other than impermissible hindsight, it is not understood would have motivated the skilled artisan to do away with that prior art requirement and merely detect the malicious code without notifying an administrator or security personnel. The Examiner must indicate some **reason** for concluding that it would have been obvious to eliminate “in response to detection of an instance of malicious code, generating and transmitting an event indicating the detection to a security manager” from the claims of the co-pending application. The Examiner has merely set forth the conclusion of obviousness without providing a cogent rationale for reaching that conclusion.

Accordingly, since the Examiner has failed to establish a *prima facie* case of obviousness with regard to instant claims 1, 3, 5, 8, and 10, and because the instant claimed subject matter is patentably distinct over claims 1, 4, 7, 11, and 14 of co-pending application 10/024,202, because the instant claims do not require a security manager to be notified every time a malicious code is detected, the rejection of these claims under obviousness-type double patenting must be reversed.

B. CLAIMS 1, 3, 5, 6, 8, AND 10-15 ARE NOT RENDERED OBVIOUS BY HYPPONEN ET AL. AND YANOVSKY BECAUSE HYPPONEN ET AL. AND YANOVSKY FAIL TO PROVIDE FOR THE CLAIMED “PLURALITY OF INTRANETS.”

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. *In re Mayne*, 104 F.3d 1339, 41 USPQ2d 1451 (Fed. Cir. 1997). Moreover, the Patent Office must give specific reasons why one of ordinary skill in the art would have been motivated to combine the references. See,

e.g., *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000); *In re Rouff  t*, 149 F.3d 1350, 1359, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998).

Each of the claims on appeal recites, *inter alia*, “a network security system to be deployed between a **plurality of intranets** and an internet backbone.” *Hypponen et al.* only shows one computer data network 1, in addition to the Internet 5, and has no disclosure of a “plurality of intranets,” much less a “scanning system coupled to the intranets,” as claimed. The computer data network 1 comprises a wired or wireless network 3. While the latest Office Action of November 2, 2007 again relies on the network (presumably network 1) of *Hypponen et al.* as an “intranet,” the present claims require a “plurality of intranets.” *Hypponen et al.* lacks any teaching of a “plurality of intranets” and of a scanning system “coupled to the intranets” as well as an anti-virus server “coupled to the intranets.” *Yanovsky*, cited for an alleged teaching of an internet access module for updating anti-virus protection on network devices by periodically updating network devices (column 1, line 66 –column 2, line 11) (see the Office Action of November 2, 2007 – pages 3-4) fails to provide for the “plurality of intranets” missing from *Hypponen et al.* Accordingly, no *prima facie* case of obviousness has been established.

The Examiner contends that *Hypponen et al.*

discloses plurality of users (figure 1:2a-2d and [0031]), although they are connected through network 3, one with ordinary skill in the art would understand that each **could** be connected to another intranet to form plurality of intranets. Therefore, the idea of expanding the security system from one intranet to plurality of intranets does not render the application novel from prior art of record. [sic](Office Action of November 2, 2007-page 8, emphasis added).

The Examiner’s rationale is flawed in various aspects. First, even if an intranet in *Hypponen et al.* **could** be connected to another intranet to form a plurality of intranets, as claimed, this is not the proper test for obviousness, within the meaning of 35 U.S.C. §103.

Certainly, a plurality of intranets **could** be connected, because Appellants have done so. However, the test for obviousness, within the meaning of 35 U.S.C. §103, is not whether something **could** be done but, rather, by what a reference or combination of references would have suggested to those of ordinary skill in the art. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Keller et al.*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

There is nothing within the teachings of *Hypponen et al.* or *Yanovsky* that would have suggested a network security system deployed between a **plurality of intranets** and an internet backbone. Each of the users 2 in *Hypponen et al.* is connected to the same network 3. Thus, even if one considers network 3 to be an intranet, there is only a single intranet disclosed by *Hypponen et al.*, and not the **plurality of intranets** required by the claims on appeal.

Second, the Examiner states that the idea of expanding the security system from one intranet to plurality of intranets does not render the application **novel** from prior art of record. To the contrary, the Examiner has already admitted the claimed invention is **novel** by not finding the claimed connection of a plurality of intranets in the applied prior art. The question before this Honorable Board is one of obviousness under 35 U.S.C. §103, not one of novelty under 35 U.S.C. §102. In particular, the issue is whether it would have been obvious to modify the teaching of *Hypponen et al.* to deploy a network security system between a **plurality of intranets** of respective organizations and an internet backbone, wherein a single scanning system and a single anti-virus server is coupled to **the plurality of intranets** for scanning incoming electronic mail for malicious code, and for downloading anti-virus code to clients coupled to the intranets, respectively.

Appellants respectfully contend that it would not have been obvious to so modify *Hypponen et al.* since *Hypponen et al.* does not teach or suggest the claimed **plurality of**

intranets and a **single scanning system** and a **single anti-virus server** coupled to that **plurality of intranets**. *Hypponen et al.* does disclose a centralized virus scanning process at paragraph [0011], but it is not connected to a **plurality of intranets**.

Further, the Examiner identifies paragraphs [0012] and [0013] of *Hypponen et al.*, as well as Figure 1, as disclosing a switch, yet no switch is shown in Figure 1. The cited paragraphs are directed to a “transit node,” disclosing how it may be a gateway coupling the network to an external system or network. This transit node may be a database server, an electronic mail server, an Internet server, a proxy server, or a firewall. However, no mention is made in *Hypponen et al.* of the transit node being a switch. In any event, there is no disclosure or suggestion of a switch “coupled between the internet backbone, the scanning system, and the anti-virus server” and being configured for “directing incoming electronic mail from the internet backbone to the scanning system.”

Moreover, *Yanovsky* does not provide for any of these deficiencies of *Hypponen et al.* The Examiner employs *Yanovsky* for a teaching of an internet access module for updating anti-virus protection on network devices by periodically updating network devices, citing col. 1, line 66-col. 2, line 11. The Examiner then concludes that it would have been obvious “to utilize the internet access module/anti-virus server and the scanning server as an anti-virus system to be coupled to a transit node/switch because providing virus scanning and virus code update are well known features of anti-virus systems and both prior art discloses protection of local area network/intranets”[sic] (Office Action of November 2, 2007-page 4).

While *Yanovsky* teaches a method and system for administrating and managing anti-virus protection on a local area network, this teaching, in no way, provides for the deficiency in

Hypponen et al. in failing to suggest a network security system deployed between a **plurality of intranets** and an internet backbone.

By using a network security system deployed between a **plurality of intranets** and an internet backbone, Appellants are able to provide economies of scale that the prior art of record could not provide, because Appellants' network security system is shared between various organizations. This is an important contribution that is not disclosed or suggested by the applied references. Appellants should not be denied a patent on the Examiner's unsupported allegation that each of the users (workstations, servers, and administrators 2a-2d) in *Hypponen et al.* "could potentially serve in another intranet," and that it would have been obvious "to apply the intranet anti-virus system to plurality of intranets to reduce the cost of implementing a separate system for each intranet" [sic] (Office Action of November 2, 2007-page 4). It is Appellants who have reduced the cost of implementing a separate system for each intranet, and it is impermissible hindsight for the Examiner to assert, after the fact of Appellants' invention, that it would have been obvious to do so, without any evidence supporting that allegation.

C. CLAIMS 2, 4, 7, AND 9 ARE NOT RENDERED OBVIOUS BY *HYPPONEN ET AL.* AND *YANOVSKY* IN VIEW OF *NAI* BECAUSE *HYPPONEN ET AL.*, *YANOVSKY* AND *NAI* ALL FAIL TO PROVIDE FOR THE CLAIMED "PLURALITY OF INTRANETS" AND THE CLAIMED "DECOY SERVER" IN COMBINATION WITH THE PLURALITY OF INTRANETS

NAI is cited in the rejection of claims 2, 4, 7, and 9 under 35 U.S.C. §103 as disclosing a decoy server used to trace and track hackers and reporting all intrusive activities to security administrators.

First, the subject matter of claims 2, 4, 7, and 9 is not obvious for the reasons *supra*, because *NAI* fails to fill in the gaps left by *Hypponen et al.* and *Yanovsky* regarding the claimed **plurality of intranets**.

Moreover, the artisan of ordinary skill, upon reading *NAI*, would be led to believe that a decoy server would be necessary for each network being protected. Thus, at best, the skilled artisan seeking to modify *Hypponen et al.* with the teaching of *NAI* would apply a single decoy server in the single intranet of *Hypponen et al.* There is, however, no disclosure or suggestion in any of the applied references of modifying *Hypponen et al.* by using a plurality of intranets and applying a single decoy server coupled to the plurality of intranets, as positively recited by claims 2, 4, 7, and 9.

Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness and the Honorable Board is respectfully requested to reverse each of the Examiner's rejections under 35 U.S.C. §103

VIII. CONCLUSION AND PRAYER FOR RELIEF

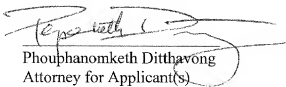
For the foregoing reasons, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

11/24/07

Date


Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax. 703-519-9958

IX. CLAIMS APPENDIX

1. A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the scanning system.

2. A network security system according to claim 1, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

3. A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

- a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;
- a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to the scanning system when the incoming electronic mail is determined to be scanned for malicious code;
- an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and
- a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:
 - directing incoming electronic mail from the internet backbone to the mail proxy server.

4. A network security system according to claim 3, further comprising:

- a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;
- wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

5. A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code;

a plurality of anti-virus servers coupled to the intranets for downloading anti-virus code to clients coupled to the intranets;

a plurality of switches coupled between the internet backbone, the scanning systems, and the anti-virus servers, said switches configured for:
directing incoming electronic mail to at least one of the scanning systems.

6. A network security system according to claim 7, wherein the switches are further configured for:

load-balancing among the scanning systems and among the decoy servers.

7. A network security system according to claim 5, further comprising:

a plurality of decoy servers coupled to the intranets for masquerading as legitimate servers and logging activity on communications received via the internet backbone;

wherein the switches are further coupled to the decoy servers and are further configured for redirecting suspicious traffic from the internet backbone to the decoy servers.

8. A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to a scanning system;

scanning incoming electronic mail for malicious code; and

downloading anti-virus code to clients coupled to the intranets.

9. A method according to claim 8, further comprising:

redirecting suspicious traffic from the internet backbone to the decoy server;
simulating the decoy server as a legitimate server to the suspicious traffic; and
logging activity on communications received via the internet backbone.

10. A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to one of a plurality of mail proxy servers;
at the one of the mail proxy servers, determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to a scanning system when the incoming electronic mail is determined to be scanned for malicious code;
at the scanning system, scanning incoming electronic mail for malicious code;
downloading anti-virus code to clients coupled to the intranets.

11. A method according to claim 10, further comprising:

load-balancing among the mail proxy servers.

12. A network security system according to claim 1, further comprising:

a hub in communication with the scanning system and the intranets, wherein the scanning system is further configured for sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets and directing the sanitized incoming electronic mail to the recipients via the hub.

13. A network security system according to claim 3, further comprising:

a hub in communication with the scanning system and the intranets, wherein the scanning system is further configured for sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets and directing the sanitized incoming electronic mail to the recipients via the hub.

14. A method according to claim 8, further comprising:

sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets; and
directing the sanitized incoming electronic mail to the recipients on the intranets.

15. A method according to claim 10, further comprising performing, at the scanning system, the steps of:

sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets; and
directing the sanitized incoming electronic mail to the recipients on the intranets via a hub in communication with the scanning system and the intranets.

X. EVIDENCE APPENDIX

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI. RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.